July 17, 2003

CDR Bob Hennessy

Re: CTAC Comments/Recommendations to Security Interim Rules

On behalf of CTAC, I am attaching a copy of the comments generated by our membership in regards to the interim final rules of maritime security. The CTAC Subcommittee on Security met on July 15 and 16, 2003 to develop a draft of comments and questions. The comments were reviewed and edited by the full CTAC membership on July 17, 2003. Once finalized, the committee voted to accept the comments, which we are now submitting for your consideration.

In conducting our review, we did identify several issues that could have a major impact on our industry. While we have included a discussion of these issues within our comments, we feel the need to point these out early so that they take a high priority for review within the Coast Guard. As always, CTAC and our security subcommittee are ready to assist the Coast Guard in working through these issues to find a solution that provides for the safety and security of our industry and the public while still enabling the free flow of commerce. These issues include:

- There currently exists a critical gap in the communications process the Coast Guard is using to convey information on the Maritime Security (MARSEC) Level to these stakeholders. A practical, effective communications system between the Coast Guard and the maritime community is essential to ensuring maritime security.

- There is significant confusion related to the definitions of “vessel-to-vessel activity” and “vessel-to-facility” interface, and in particular, how this relates to the requirements for the use of the Declaration of Security in the unmanned barge industry. If the Coast Guard intends for the industry to complete a DOS each time a vessel is handed off to another vessel or a facility, this will have significant ramifications on the industry, while, in our opinion, not enhancing the security of those activities.

- The inland tank barge industry will face major difficulties in complying with the regulations as written. This particular area would be well served by forming a working group of industry representatives to review the regulations and develop practical solutions that would provide for suitable security while enabling the industry to continue operating in a reasonable fashion.

- The committee feels strongly of a need to develop an “outreach” process to stakeholders in the interim final rules. The interim final rules, as they are important to securing the maritime industry, are probably the most far-reaching regulation to impact the maritime industry. The short implementation timeline, complexity of reading and interpreting the rules, writing plans and training in accordance with, is a challenging task to be addressed by the stakeholders and also the U.S. Coast Guard. The committee believes an outreach process would beneficially save time and effort. As always, the CTAC committee and subcommittee of security are willing to assist in this “outreach” need.

I would like to emphasize the amount of effort that CTAC and the subcommittee has put into developing these comments. We must also acknowledge the outstanding involvement of the US Coast Guard and Army Corps of Engineers. Without the efforts of all those who participated, this work product would not have been possible.

The CTAC membership, and the members of the subcommittee, serve to represent most facets of our industry with a wealth of knowledge and experience. If you find it necessary to solicit assistance in identifying workable solutions to some of these issues, we can quickly form working groups that tap into this knowledge and represent the impacted segments of the industry.

Paul Book, …..

Implementation of National Maritime Security Initiatives (Part 101 et al.)

101.105 – Definitions:

1. Barge fleeting facility – There are fleeting areas that are provided by the Corps of Engineers for making and breaking tows, or for temporarily staging vessels (i.e. when passing through a lock). In most cases, these are unmanned, so the towing vessel always maintains custody of the vessel. They do not seem to fit the definition of a "barge fleeting facility" since they are not a "commercial fleeting area". The definition in 105.105(a)(4) is more general and could include these facilities, but doesn't necessarily match the definition in the general section. As such, we recommend that government-provided moorings, such as fleeting facilities and anchorages, should be incorporated into the Area Security Plan.
2. Certain Dangerous Cargo - At this point, it is difficult for a company to determine if a particular cargo is a CDC, particularly when dealing with mixtures. The USCG has an in-house list of products that would fall into the list, but this is currently considered Security Sensitive Information (SSI). At this point, it is up to each company to determine if the cargoes they handle are CDC's by referring to the definition and the lists in 46 CFR 154.7. If possible, the Coast Guard should develop a process so that this list can be released to the industry. In addition, CTAC will be working with the Coast Guard to identify mixtures that might fit the criteria as a CDC.
3. Vessel-to-vessel activity - Per the USCG, "goods" in the definition of "vessel to vessel activity" is intended to include cargo. This is unclear, and will be misinterpreted by industry. We recommend that the definition be modified to state "… cargo and goods…" to prevent this problem.
4. Waters subject to the jurisdiction of the U.S. – What does the term "superadjacent" mean?

101.120 – Alternatives:

5. In (a)(2)(b), facilities that serve only vessels on international voyages are excluded from using an alternative security program. However, by simply bringing in one vessel on a domestic voyage, it seems that the facility could then use the program. Why are facilities that only see vessels on international voyages excluded?

101.200 – MARSEC Levels:

6. Per the USCG, if the DHS goes to a heightened threat level on a national level, the Coast Guard will most likely raise the MARSEC level to match. However, if the DHS threat level is only raised for a particular area or segment of the industry, only those affected parts of the maritime industry

would be elevated. It is difficult for companies to elevate in one particular area but not in others (i.e. the main facility and rail area elevate based on DHS level, but docks and barges calling on that facility don't face an elevated MARSEC level). The typical delay that we see from the time DHS changes the level until the MARSEC level is changed is also creating problems. The Coast Guard needs to develop a system that allows maritime interests to obtain timely information about changes in the MARSEC Level from their respective Captains of the Port. The need for such a system is now even more acute since the interim rules on maritime security, which require companies to scale their security operations based on the current MARSEC Level, have been published. We encourage the Coast Guard to look to the effective communications processes already implemented in several ports, including Houston and New York, as models for the rest of the maritime community.

101.305 – Reporting:

7. Industry is concerned that the use of the National Response Center may create a bottleneck given the current use of the number for other responses including pollution.

101.405 – Maritime Security Directives:

8. (a)(2) refers to a "covered person" as a term that is defined in 49 CFR 1520 related to SSI. However, upon review of those regulations, we did not find a definition for a "covered person" in those regulations. Could the USCG define who a "covered person" is?
9. A variety of issues have been identified related to Maritime Security Directives, many of which hinge on the communications protocols as previously discussed. For example, since these directives are classified as SSI, companies that operate in various COTP Zones have to send people to hand pick-up new directives at each of those COTP offices. This is impractical, especially when some COTP's may publish new directives in response to a particular threat, and expect actions to be put in place within a short time period.
10. Some of the recommendations related to directives:
    - Whenever possible, directives should be standardized across the US.
    - MARSEC levels should not be communicated through directives. The current MARSEC level must be widely disseminated throughout the industry.
    - The Coast Guard must develop a process for providing directives out to the industry in a streamlined fashion. Some of the ideas offered include:

- Allow companies to submit an “SSI form” on a national level, rather than COTP office by office.
- Have MSO’s keep directives from all MSO’s available so that each MSO serves as a one-stop shop for directives.
- Arrange a secure web site where individuals with SSI authorization can access the directives from all COTP zones.

101.300 – Preparedness communications:

11. Communications by COTP will be through various means that should be covered in the AMSP (Area Maritime Security Plan). The COTP should communicate security conditions to vessels that have submitted an ANOA via NAVTEX, NTM, etc.

101.305 – Reporting:

12. This section contains provisions for reporting suspicious activities, breaches of security, and TSI’s. However, in many cases, the first notification is to the National Response Center (NRC), which will not provide for the quickest response. In any of these cases, the process used for other types of response, such as environmental incidents, would provide for a quicker activation of resources and help minimize the potential impact. The normal course of action should be to:
    - First, activate your security plan and when necessary, your response plan (i.e. shut down operations, evacuate if necessary, etc.);
    - Second, notify local law enforcement;
    - Third, Notify the local COTP
    - Fourth, notify the NRC “as soon as practical”.

101.510 – Assessment tools:

13. Provided your assessment tool complies with the criteria listed in the appropriate section, a company can use that tool (i.e. for vessels, see 104.305).

Vessel Security (Part 104 et al.)

104.115 – Compliance Dates:

1. In (a), make a clear distinction between U.S. and Foreign Flag carriers when requiring plan submittal to the Marine Safety Center (MSC). The purpose for this distinction is necessary in order to:
   - Prevent unintended interpretation which could advance the compliance date for vessels under 104.105(c) to 29 December 2003;
   - Clearly establish that security plans for vessels under 104.105(c) should not be sent to the MSC.

104.120 - Compliance Documentation:

2. In (a)(4), wording as to the applicability of compliance with ISPS Code Part B is vague. Subpart B of the ISPS Code is required for international vessels calling US ports, but is only recommended internationally.

3. In (b), the owner or operator is required to have the plan or program available upon request by the Coast Guard. The Coast Guard should clarify what a "scheduled inspection" is, and what the expectation is for providing the VSP to the location of the inspection. It will be impractical, and could also pose a security risk, if the owner is forced to send a copy of the VSP to the shipyard or other location each time a vessel might be inspected.

104.145 - Maritime Security Directive:

4. See our earlier comments related to the communication of these directives to the industry.

104.210 - Company Security Officer:

5. In (a)(4), there should be a provision for the CSO to have a formal alternate when he is not available due to vacation, illness, etc.

104.215 - Vessel Security Officer:

6. (a)(3) requires that if a person serves as the VSO of more than one unmanned vessel, the name of each vessel that he is the VSO for must be listed in the VSP. In the inland tank barge industry, it will likely be better to allow the Master of the towboat serve as the VSO when that barge is under his control. Due to the dynamic nature of inland tank barge operations, actual listing of the barges assigned to the boat or particular VSO in the Vessel Security Plan is not practical. We need a provision to handle the temporary barge assignments given to the boat.

104.225 - Security Training for All Other Vessel Personnel:

7. The level of security training for temporary contract repair or other service personnel who board the vessel for authorized work is too extensive. Was it the intent that the training requirements are for crewmembers, temporary or permanent, and contractors sailing with the vessel or for every authorized person who boards the ship? If the intent was every person, 104.225 (c), (d), and (e) require too much info to cover for shoreside temporary repair contractors or terminal employees going onboard a vessel.
8. Would it be possible to develop a standard brochure or similar aid that could be used to provide appropriate training or orientation for other vessel personnel, such as contractors, etc? This may also be addressed by the Transportation Worker Identification Card (TWIC) program, since those with a TWIC may have to have some security training.
9. Personnel who will be performing security duties, such as a Vessel PIC or a crewmember, should require security training. Personnel who are only on the vessel to perform work and that will not perform security duties should simply require an appropriate orientation program related to security awareness and reporting.

104.230 – Drills:

10. (b)(1) requires quarterly drills. While this is reasonable for manned vessels, it is totally impractical on unmanned tank barges. In addition, if drills are conducted within the same class of towing vessels/manned barges covered by a common VSP, this should validate individual crewman drill requirements within that common class of ships. This will help with the 25% rule for new but experienced crewman reporting aboard.
11. The exercises for towing vessels required in (c) should be driven or executed by the CSO. The exercise requirement should be on a company wide basis. Towing vessels/tank barges should be included in exercises run by the CSO with VSO & crew involvement. Mandating that every vessel run exercises is not practical. Drill the vessels. Exercise the management and the system.
12. We need a clarification of the terms “full scale” or “live” in (c)(2)(i). In addition there is no mention for a real security incident or reaction to a threat validating the drill or exercise requirement.
13. In (c)(2)(ii), add “Computer Simulations” as another option.

104.235 - Vessel Recordkeeping Requirements:

14. Recordkeeping requirements as required in (a) should be specified as limited to manned vessels.

15. The recordkeeping requirement in (b)(4) does not exclude unmanned tank barges. This requirement should be limited to the Manned Vessels, Fleet, or Facilities.
16. (b)(7) requires that manned vessels maintain DOS records while unmanned vessels are not mentioned, so this is interpreted to mean that unmanned tank barges will have its security maintained by an approved VSP or FSP. The unmanned tank barges need not be manned just to keep security records. Manned vessels, facilities, or fleets will maintain security or surveillance and the records unless otherwise provided.
17. (c) requires that the records "must be protected from unauthorized access or disclosure". Could the USCG clarify if this information is considered SSI? In addition, there is no suitable place on an unmanned vessel to maintain these records in such a way that they would be protected in this manner.

104.240 - MARSEC Level of Coordination and Implementation:

18. It would be beneficial to clarify (b)(2): Does this paragraph indicate that only manned vessels will be calling when in compliance? Since facilities and barge fleets have control over unmanned vessels moored in their locations, it is assumed that the FSO will report that the unmanned tank barges are in MARSEC Level 2 status in accordance with the FSP.

104.255 - Declaration of Security (DOS):

19. In (b)(1), (b)(2), and (c), we recommend that the security arrangements be arranged "ON OR PRIOR TO" rather than "PRIOR TO". For facilities/vessels that have been conducting DOS's already, this has been working successfully. In many cases, it could be difficult to arrange for security needs "prior to arrival", especially when some of these directives will be provided by Immigration or the USCG after the vessel arrives at the berth, or when the rotation of the vessel is changing.
20. (b),(c),and (d) - MARSEC Level 1, 2, and 3 requirements are not consistent. At some times, the DOS must be implemented "prior to an interface", while at other times, it is "prior to cargo transfers". Also, please see the previous comment.
21. It is recommended that (e) be moved up to (c), and (c) and (d) moved down respectively.
22. In addition, in (e), it might be worthwhile to clarify the paragraph by stating "When required to complete a DOS at MARSEC Levels 1 and 2, VSO's of vessels…". The concern is that some vessels are not required to complete a DOS at MARSEC 1, but the wording might be interpreted to require one.

104.265 - Security Measures for Access Control:

23. Insert the word “manned” into (a) so that it reads “The manned vessel owner…”, as this would be difficult for the owner to oversee on unmanned vessels. Another alternative would be to indicate “as appropriate”. The issue is that many of these requirements do not fit the unmanned vessel industry since there is no person onboard the vessel at most times.
24. Posting signs as indicated in (e)(2) on unmanned tank barges must be excluded.

104.290 - Security Incident Procedures:

25. In (a)(1), change “Prohibiting” to “ Deter to the best of their ability “.
26. In (a)(2), change ”Deny” to “Denying access to the best of their ability”.

104.410 - Submission and Approval:

27. In (a), insert “each vessel owner or operator ‘where required’ must either…”.
28. On page 39294 of the Vessel Security Rule, the Interim Rule Discussion of “Alternative Security Program” states in paragraph two that Vessel Security Plans constructed using a model plan would still require submission for approval by the Coast Guard. However, 104.410(a)(2) states “If implementing a Coast Guard approved Alternative Security Program, meet requirements in 101.120(b) of this subchapter”. In 101.120(b)(3), it is stated “Owners or operators who have implemented an Alternative Security Program must send a letter to the appropriate plan authority under part 104, 105, 106 of this subchapter …”. Please clarify this difference in the discussion and the regulation wording. Does the company submit its whole VSP, SVA, and security audit to the USCG no matter which path it takes to implement a VSP?

160.206 – Information required in an NOA:

29. Text should be added that would establish this as a temporary regulation that will sunset 5 years after implementation, and in addition, the SOLAS ISM certifications should be sunset, with the NOA regulations being deleted for the SMC and DOC. All affected vessels will have been through the first “regulatory cycle” by this date requiring that they have all documents necessary to trade to the US. New vessels or vessels calling on the US for the first time will be inspected per the normal LOC or TVE process.

105 – Facility Security

105.105 – Applicability:

1. Questions still arise about when a facility is or is not regulated. The group has attempted to show various types of facility layouts (See Attachment #1 at the end of the Facility section), and based on our discussions, identify which are or are not regulated. It might be helpful for the USCG to review these examples to insure we are correct, and then share this information throughout the industry.
2. Questions arose whether an isolated 127 facility (LHG) could be exempted from applicability per (a)(5). The answer is no per 105.105(a)(5).

105.110 – Exemptions:

3. Fleeting facilities are exempted from security measures for delivery of vessel stores and bunkers. At some fleeting areas, provisions are put onboard vessels, surveyors collect samples, and equipment and repairs are completed. As such, allowing this exemption would serve as a weak point in the system. To prevent this, fleeting facilities should have adequate security to include inspection/oversight of all materials/personnel coming in or going out.

105.145 – Directives:

4. As a general comment, requirements in a directive will include “will” and “shall” rather than “may” or “should”. However, allowances in many cases should be granted for equivalent methods.

105.200 – Owner or operator:

5. (b)(8) requires that facilities implement within 12 hours of notification. This could be a problem on weekends or nights. It is also a problem since at many facilities, the FSO will not be a marine-based individual. This item needs to be discussed further as communications protocols are reviewed.
6. (b)(2) requires that facilities have a designated FSO. 105.205(a)(3) allows companies to delegate responsibilities to others. Can there be designated “alternate” FSO’s to cover when the primary FSO is unavailable?

105.210 through 105.215 – Facility personnel with security duties & Security training for all other facility personnel:

7. The regulations only require that facility personnel meet certain training or knowledge. However, the preamble indicates that these may change in the future. We concur with the existing requirements, and do not want to have

training requirements mandated in the future (i.e. do not require personnel to attend particular courses, etc.).

105.220 – Drill and exercise requirements:

8. Comment: There should be an allowance that companies can take credit for actual incidents or threats. This would mirror 103.515(c) that allows the District Commander to give credit when the MARSEC level is increased.

105.225 – Facility recordkeeping requirements:

9. Comment: (b)(7) requires that the DOS be retained for 90 days. Current requirements are that DOI's (Declaration of Inspection) have to be retained for 30 days. Since the DOS is an extension of the DOI, it would be better to line them up to both retain for 30 days. There is not much value to retaining the DOS for such a long time, and it will take up a lot of space on barges and at facilities.

105.230 – Maritime security level coordination and implementation:

10. (b)(1) requires that facilities notify any vessel at their facility, as well as any vessel due to arrive within 96 hours of a change in the MARSEC level of the new MARSEC level. Facilities have no problem notifying vessels that are at their facility of a new MARSEC level. It will be difficult and impractical for facilities to notify vessels 96 hours prior to arrival. Some vessels and facilities do not have a means to provide secure communications for this discussion, and in some cases, the facility will not even know how to contact the vessel until it arrives in the general area. In addition, since vessel schedules may change, or the upcoming berth may not be identified so far in advance, it will be difficult for the facility to communicate the current MARSEC level.
11. (c) requires that "all" facility personnel must be notified about threats. Personnel need to understand the current MARSEC level and have a heightened state of awareness, but in most cases, the specifics of the threat should not be disclosed.
12. (e) provides a "laundry list" of additional measures that "may be required to implement". It should be stressed that these are strictly examples.

105.235 – Communications:

13. (b) requires that there be communications between the vessel and the facility security. Per the USCG, provided that an effective means of communications is in place and documented in the facility plan, it is acceptable for the vessel to communicate to the facility PIC, and the facility PIC can then contact security.

105.245 – Declaration of Security:

14. The following table was developed to identify when DOS's were required for vessel-to-facility interface. Please see the legend that follows to assist in interpreting the requirements:

Task	Type	MARSEC 1	MARSEC 2	MARSEC 3
F/V	Manned, CDC	S/C(max 90)	S/C(max 30)	S
	Unmanned, CDC	None	S/C(max 30)	S
	Manned, Hazmat	None	S/C(max 30)	S
	Unmanned Hazmat	None	S/C(max 30)	S
	Manned, non-Hazmat	None	None	None
	Manned, non-Hazmat on an international voyage	None	S/C(max 30)	S
	Unmanned, non-Hazmat	None	None	None
	Unmanned, non-Hazmat on an international voyage	None	S/C(max 30)	S

S=Single DOS, C=Continuous DOS
(Number = maximum days continuous DOS is allowed)

15. There is significant confusion regarding the requirements to complete a DOS, especially when dealing with unmanned barges. Some individuals, as well as the Coast Guard, suggest that a DOS is required anytime the vessel undergoes a new interface, such as being dropped at a facility or changing tows. Others feel that the DOS is required only when there is some sort of transfer, such as the transfer of cargo or personnel. The make-up of the suggested DOS's seem to work for an ongoing interface, such as during a transfer. A working group was asked to review the issue and come up with a recommendation to the subcommittee (see recommendations below).
16. In particular, issues related to DOS's and unmanned barges were identified. For example, is it acceptable to appoint a VSO for unmanned barges by title, such as the Captain/Pilot of the tug, or the Vessel PIC during a transfer operation?
17. The group does not see where the use of chains of DOS's for moves between vessels and/or fleets will enhance security beyond what the existing chain of custody procedures currently provide. These requirements need to be adapted to match the way the industry operates. While we understand the need to provide for the security of the unmanned barge, the requirements must be developed in a manner that minimizes negative impact on the flow of commerce. The subcommittee has developed a draft proposal for consideration.

18. The working group as mentioned above, developed their recommendations based on the following guiding principles:

    - Unmanned barges by their very nature are “unmanned”. As such, while the security plan for the barge will define particular parameters (i.e. restricted areas, signage onboard, etc.), the vessel towing the barge or the facility where the barge is moored will be manned, and will be responsible for insuring the overall safety of the barge. In this manner, the tug or facility plan will envelop those vessels that are within their control.
    - This concept will align with the OPA ’90 practices where a tug accepts responsibility to initiate the response when an incident occurs to a barge in its tow.
    - This is also similar to our everyday activities. For example, if you have borrowed a friend’s trailer, and in the course of towing that trailer, the brake lights were not working, you as the driver of the auto in control of the trailer would be ticketed, not the owner of the trailer. The key to providing security of an unmanned vessel lies in the vessel or facility that is currently in control of that vessel.
    - The vessel that is towing the unmanned vessel, or the facility that the unmanned vessel is moored at, is in control of that vessel when it is unmanned. As such, the security of the unmanned vessel relies on the entity that has control of it. When a Vessel PIC goes onboard, that person takes over security responsibilities as defined in the VSP. A DOS should be required for interfaces where cargo, goods, or passengers are transferred, but no DOS should be required when the control of the vessel is changed, since the security aspects for that vessel will fall under the single entity that has control of it.

19. The team recommended the following:

    - Modify the definition of a “Vessel-to-vessel activity” by adding the following after the current definition:
        - A vessel-to-vessel activity includes the transfer of a container subject to the requirements in 49 CFR Subchapter C to or from a manned or unmanned vessel. The movement of an unmanned vessel to or from another vessel, such as transferring an unmanned barge from a vessel to a facility or other vessel is not considered a vessel-to-vessel activity.
    - Add the following to the vessel regulations as 104.400(a) as a new # (7):
    - For vessels towing unmanned vessels, the security plan must include:
        - The manned vessel provides for the security of the unmanned vessel under tow by that vessel;
        - No unmanned vessel under tow by the vessel may be released from the vessel to a facility or other manned vessel without the approval of the receiving facility/vessel;

- When picking up an unmanned vessel from a facility or other manned vessel, responsibility for insuring the security of that vessel commences upon “last line”, and when dropping an unmanned vessel off, ends when the unmanned vessel is all fast at the facility and the tug has released all lines from the unmanned vessel.

- Similar provisions would need to be incorporated into the facility regulations.
- For unmanned vessels, the Vessel PIC will likely be delegated some responsibilities by the VSO, such as signing the DOS and performing duties outlined in the VSP. In this case, the Vessel PIC must be suitably trained to serve in this designated capacity. It is likely necessary for the training requirements/regulations for tankermen to be updated to include security. 104.225 specifies the requirements for training of other vessel personnel, so it might only require clarification for the benefit of the industry.

20. As mentioned earlier in the Executive Summary, the use of DOS’s, particularly in the unmanned barge and towboat industry should be re-designed with the help of members of the industry in order to better meet the current operational aspects of the industry. With this type of effort, a process could be put in place that adequately provides for the security of those vessels.

105.265 – Security measures for handling cargo:

21. (a)(6) restricts the entry of cargo to the facility that does not have a confirmed date for loading as appropriate. This should be clarified to refer to break bulk and packaged cargo shipments where containers would be stored on-site while waiting for arrival of the vessel, and should exclude bulk liquid facilities.
22. 105.265(a)(9), as well as 105.265(d)(3) indicate that facilities must have an inventory of all dangerous goods or hazardous substances. It will be an expectation that this information will be shared with appropriate personnel during a TSI, which would include response personnel.
23. (b)(1) and (b)(4) require that facilities check cargo and seals that are used to prevent tampering for quality assurance or security. In some cases, health and occupational safety concerns could prevent safe access to inspect the seals onboard the vessel.

105.280 – Security incident procedures:

24. (d) requires the facility to brief all facility personnel on possible threats. Per our earlier comment, only the MARSEC condition and additional security procedures should be shared, but not the information related to the specific

threat. In addition, modify it to say “all personnel on-site”, as this would now include contractors, response personnel, government agencies, etc.

105.295 – Additional requirements – Certain Dangerous Cargo facilities:

25. (b)(2) states that companies must “continuously guard or patrol restricted areas”. Would this require personnel to be there, or would we be allowed to use electronic equipment (i.e. cameras/monitors) that is monitored by personnel to satisfy this requirement?

105.296 – Additional requirements – barge fleeting facilities:

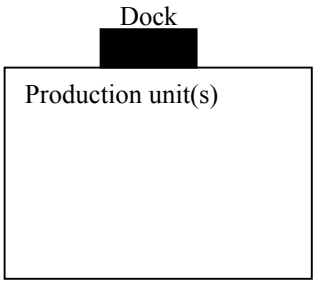
26. (a)(1) requires that a fleeting facility segregate barges carrying CDC’s and other hazardous substances. In some cases, it is probably better to keep the vessel separated so as to minimize the impact if something occurs (i.e. if multiple LHG barges are stored side-by-side, an incident on one could create an even larger incident). As such, it is recommended that the decision of how to store barges within a fleeting area be based on the results of a risk assessment. To address this, the words “If appropriate based on the results of the risk assessment, designate an area …”. Or, it might be better to be more general to address storing barges based on the risk assessment.
27. (a)(3) requires that a fleeting facility provide a towing vessel for every 100 barges within the facility. Some fleeting facilities can have up to 400 barges, but there will be multiple vessels in the area. The intent is for the tug to be “available”, which does not necessarily mean it has to be at the fleet at all times (i.e. they can be moving vessels to or from facilities or assisting tows with making/breaking tows). What is the USCG expectation?

105.400 – Facility Security Plan:

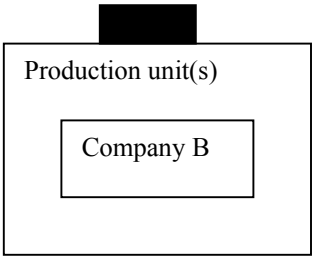
28. There is a typographical error – it currently states the section as “5.400 General”, whereas it should indicate “105.400 General”.

Attachment 1: Applicability to Different Facility Arrangements

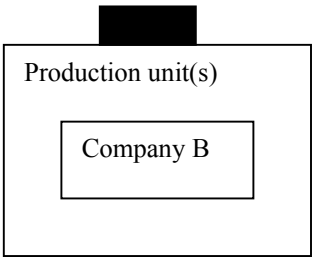
Scenario:	MTR adjacent to the production facility
Applicability:	Entire facility requires plan



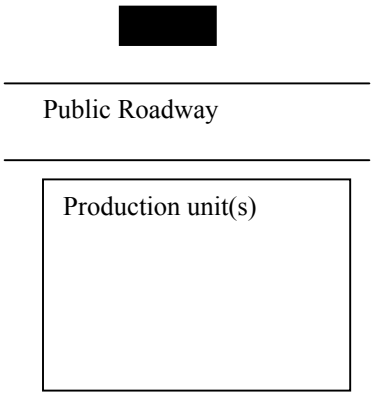
Scenario:	MTR adjacent to the production facility. Company B, a separate company, owns an operation internal to the facility, but has no MTR activities. Co. B may or may not have fencing that isolates it from the main production units.
Applicability:	Entire facility requires plan, which must consider access/egress of personnel related to Co. B activities.



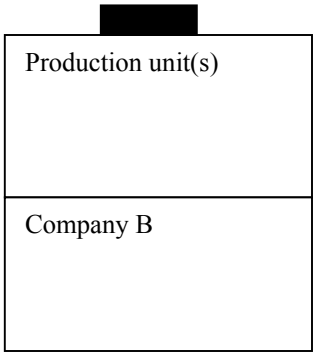
Scenario:	MTR adjacent to the production facility. Company B, a separate company, owns an operation internal to the facility. In this case, the company has MTR activities. Co. B may or may not have fencing that isolates it from the main production units.
Applicability:	Entire facility requires plan, which must consider access/egress of personnel related to Co. B activities. Company B also has to have a plan.



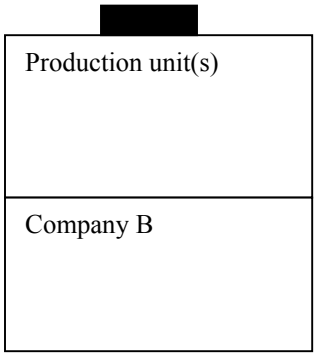
Scenario:	MTR tied to a production facility. However, the production unit is separated from the MTR facility by a public roadway.
Applicability:	Entire facility requires plan.



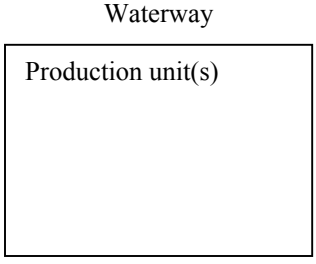
Scenario:	MTR adjacent to the production facility. Company B, a separate company, owns an operation adjacent to that facility, but has no MTR activities.
Applicability:	Company B does not fall under the regulations. The other unit does.



Scenario:	MTR adjacent to the production facility. Company B, a separate company, owns an operation adjacent to that facility, and transfers cargo to the other Production Unit, for eventual transfers to the MTR activities.
Applicability:	Company B does not fall under the regulations. The other unit does.



Scenario:	Production facility adjacent to the waterway, but no MTR.
Applicability:	Facility falls under the area plan.



Other General Issues:

CDC List:

1. Companies aware of mixtures that are shipped in bulk that contain products on the CDC list should forward a list of those cargoes to LT Mike McKean at G-MSO-3.
2. Facilities, other than fleeting facilities, that handle ammonium nitrate are regulated by the security regulations. However, vessels and fleeting areas are not. Some COTP's are concerned about these cargoes, and have implemented special requirements for vessels and facilities handling these materials. While requirements for transfer facilities will now be covered under these regulations, vessels and fleeting areas will not. This could lead to a patchwork of special requirements being developed in each affected COTP Zone. CTAC recommends that the USCG undertake a risk assessment in conjunction with this subcommittee, the AWO, the ACC, and other stakeholders to evaluate this segment of the industry. Note: Bulk Solid Hazardous Materials are listed in Subchapter N (Part 148).